DIY 第三辑

DO IT YOURSELF 自己动手做

电脑病毒的检测和防御、灭杀技巧

DO IT YOURSELF

王姿雅　罗隆福 / 编著

Hunan Science & Technology Press　湖南科学技术出版社

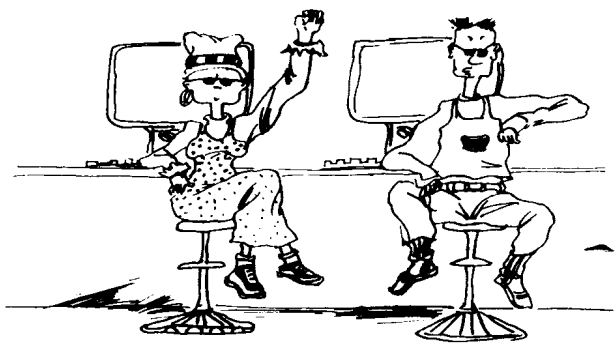
DIY第三辑

DO IT YOURSELF

自己动手做

电脑病毒的检测和防御、灭杀技巧

王姿雅　罗隆福 / 编著



DO IT YOURSELF

Hunan Science & Technology Press　湖南科学技术出版社

自己动手做丛书 · DIY 第三辑

电脑病毒的检测和防御、灭杀技巧

编　　著: 王姿雅　罗隆福

策划编辑: 罗　蕾

文字编辑: 罗　蕾

出版发行: 湖南科学技术出版社

社　　址: 长沙市湘雅路 280 号

http: //www.hnstp.com

邮购联系: 本社直销科 0731-4375808

印　　刷: 湖南省化工地质印刷厂

(印刷质量问题请直接与本厂联系)

厂　　址: 长沙市青园路 4 号

邮　　编: 410004

经　　销: 湖南省新华书店

出版日期: 2001 年 10 月第 1 版第 1 次

开　　本: 889mm × 1194mm　1/32

印　　张: 2.375

书　　号: ISBN 7-5357-3375-1/TP · 157

定　　价: 8.00 元

序言

您的电脑有没有感染过病毒？硬盘数据丢失、重要文件被破坏，甚至是硬件设施遭损坏，一定让您受够了吧。如果你的机器从没感染过病毒，也千万别掉以轻心，要知道各种病毒是无处不在、层出不穷，而且毒性还越来越大，因此一定要有防患于未然的意识哦。

本书详细地向您介绍一些常见的计算机病毒发作时的症状及其危害，以及最简单有效的解决办法，从而使我们的计算机变成病毒的禁地。让“红色代码”、“欢乐时光”、“梅莉莎”、“小天使”等披着各色漂亮外衣的病毒妖魔都见鬼去吧!

目录

1.计算机病毒概述

随着计算机应用的日益普及，计算机病毒也变得几乎是无孔不入，成为很多计算机用户的噩梦。所谓的计算机病毒是指某些人利用计算机软、硬件固有的局限性而编制的能够破坏计算机功能或者破坏数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码，它们都具有隐蔽性、复制性和破坏性。

在计算机的发展历史上，第一个被称作病毒的程序是由Fred Cohen博士于1983年11月研制出来的，运行于VAX11/750计算机系统上，可以复制自身的破坏程序。这是人们在真实的实验环境中编制的一段具有历史意义的特殊代码，使计算机病毒完成了从构思到构造的飞跃，人们的好奇心和表现欲得到了极大的满足。从此，计算机病毒开始像生物病毒一样，以其特有的方式迅速蔓延开来，对计算机的安全构成了极大的威胁，同时也给计算机技术的发展提出了新的课题。

计算机病毒的产生并不是由于突发或偶然的原因，而是一种别有意图的代码，它设计精巧，组织严密，与特定的系统或网络环境相适应，以完成预期的功能。可以说它是计算机技术和以计算机为核心

的社会信息化发展到一定阶段的必然产物。

计算机病毒的类型根据不同的角度可分为多种：按传染方式可分为引导型病毒、文件型病毒和混合型病毒；按连接入侵方式可分为源代码型病毒、入侵型病毒、操作系统型病毒和外壳型病毒；按病毒存在的媒体可分为网络病毒、文件病毒和引导型病毒；按表现性质可分为良性病毒和恶性病毒；按寄生方式可分为内存宿主型病毒和磁盘宿主型病毒；根据病毒的破坏能力可分为无害型病毒、无危害型病毒、危险型病毒和非常危险型病毒等。

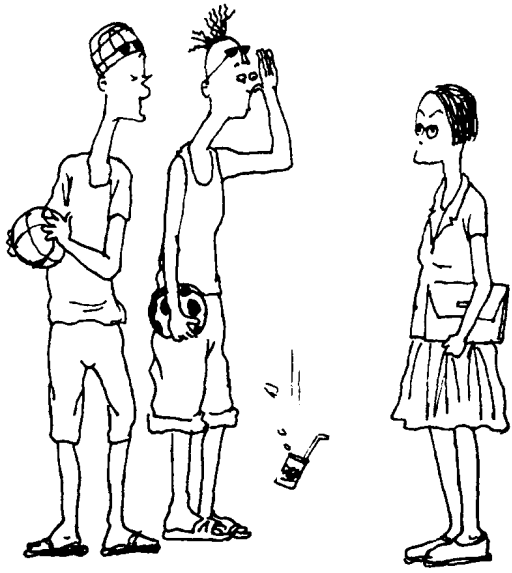
虽然计算机病毒种类很多，但是它们的主要结构却是类似的，都有共同的特点：其代码一般都很短小，但却都包含三个部分：引导部分、传染部分和表现部分。它们从功能上相互独立，但又相互关联，构成病毒程序的整体。

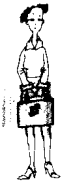
当计算机病毒发作时，其表现症状因具体病毒程序的实现过程不同而表现出多样性，但从其运行机理和目前所知的计算机病毒的总体情况来看，其共有特性是：

* 由于病毒进入内存后要不断地进行病毒传播和发作条件的判断，从而导致系统运行速度减慢。
* 病毒程序附加在可执行程序的末尾，使文件长度增加。
* 病毒程序驻留内存，造成用户可用内存空间变小。
* 用户执行无须访问硬盘的操作，但硬盘指示灯依然闪烁。
* 由于病毒程序在传染或发作过程中有意或无意地破坏了硬盘

中的有效数据，从而导致了系统的死机现象。

* 用户并未对硬盘进行写操作，但系统经常出现“写保护错”提示信息。
* 在排除硬件故障的情况下，打印机无故不联机。
* 显示屏上出现一些杂乱无章的显示内容。
* 磁盘上出现了用户不能识别的文件。
* 系统出现文件分配表错的提示信息。
* 批处理文件命令 COMMAND.COM 被修改。
* 硬盘不能引导系统。
* 磁盘上的文件内容被修改。
* 磁盘上的文件突然消失。
* 用 DIR 命令显示软盘中的文件目录时，后一张软盘的显示结果和前一张软盘相同。





2.常见计算机病毒的破坏性

近年来经常出现的计算机病毒大致是宏病毒、Windows NT病毒，另外也有一些其他的病毒如蠕虫病毒、贺卡病毒、逻辑炸弹和特洛伊木马病毒等都对个人计算机和计算机网络造成了巨大的危害。

宏病毒中的Melissa（美丽杀手）是第一个通过用户邮件通信录中的地址向外传播的病毒，它是彻底的互联网生存病毒，感染对象是Word系统。病毒发作时，它会以发送邮件的计算机主人的名义告诉被入侵者“**这是来自某某的重要信息**”，如果打开附件中名为List.doc的Word文档，不仅会看到80个色情网站的列表，而且病毒会疯狂占用系统资源，有可能造成网络的瘫痪！

WM8.autoexecbat（七月杀手）是另一个常见的宏病毒。发作时间是七月的每一天，发作时要用户在编辑文字对话框中单击“**确定**”，如果连续三次选择“**取消**”病毒将会修改批处理文件命令autoexec.bat，写入代码DELTREE /Y C:，当用户再次启动时，将删除系统盘下的所有文件，给用户的数据文件造成巨大的损失。

而蠕虫病毒则是一种在网络上传播的计算机病毒。和普通的计算机病毒相反，蠕虫的传播不需要人的干预，在很短的时间内，它可以感染大量计算机，使网络瘫痪！1988年Robert T.Morris曾

利用系统漏洞编写蠕虫病毒，在几个小时内使美国6000多台计算机瘫痪!

除了上述的种种破坏计算机系统的病毒外，近年来还出现了破坏硬件的CIH病毒、红色代码病毒和欢乐时光等病毒。此类病毒基本上是通过网络或盗版软件感染Windows操作系统，它有多个版本，病毒发作时有可能破坏计算机硬件，特别是主板和硬盘，对用户造成极大的威胁。

当我们在自己的电脑中发现了有病毒感染的症状的时候，最好的办法就是用杀毒软件处理，下面我们将首先介绍一下在Windows操作系统安装下安装KILL系列杀毒软件的环境要求和具体安装步骤。

在Windows操作系统下安装KILL 2000的软、硬件环境要求是:

机器类型——80486 DX 66MHz 或更高

操作系统——Windows 95/98/2000

系统内存——8MB或更多

磁盘空间——8MB或更多

3.KILL2000 的安装

在合适的环境下安装KILL 2000的步骤是：

（1）启动Windows 95/98，将包含该软件的光盘插入光盘驱动器。

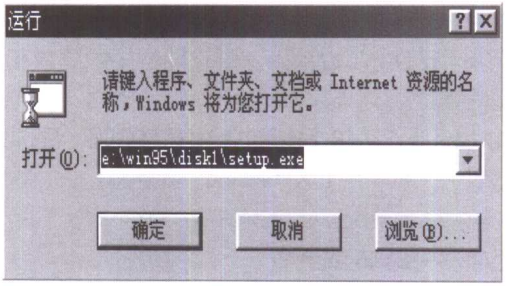


图1　运行KILL安装程序

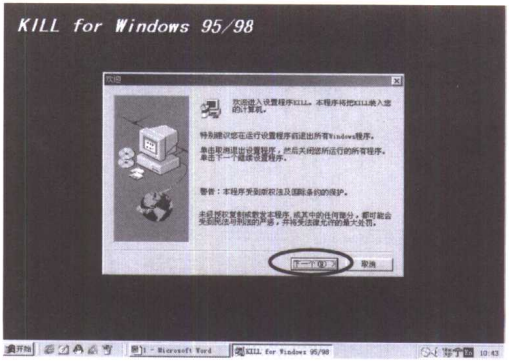


图2　KILL安装向导

（2）单击“**开始\运行**”，弹出如图1所示的对话框，在弹出的对话框中填入“**光驱盘符\Win95\disk1\setup.exe** ”，单击“**确定**”，即可启动安装向导，如图2所示。

（3）单击图中的“**下一个**”按钮，可以看到如图3所示的“**软件许可协议**”，单击“**按钮**”，在弹出对话框中输入序列号，将弹出“**用户信息**”对话框，如图4所示。

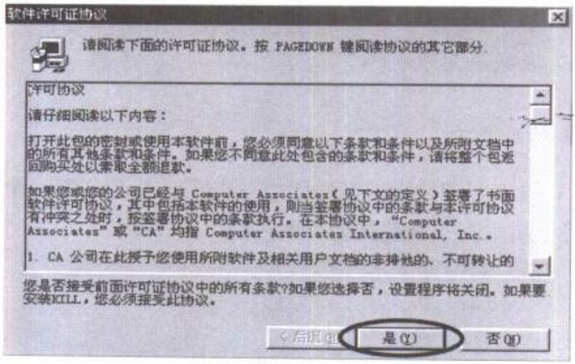
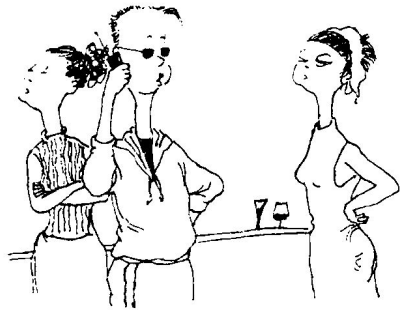


图3 软件许可协议



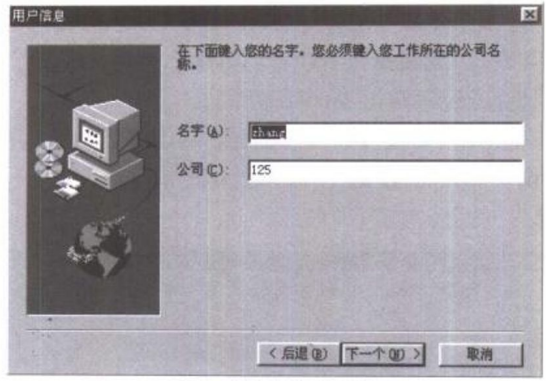


图 4　用户信息对话框

（4）输入用户信息，或使用默认信息，单击“**下一个**”按钮，弹出如图5所示的“**设置类型**”对话框。

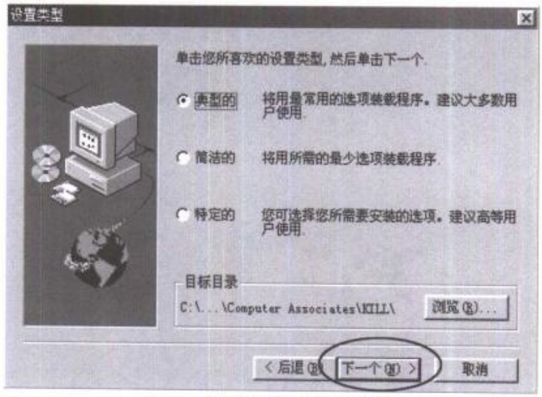


图 5　设置安装类型对话框

（5）选择安装类型（建议使用典型安装），指定安装路径（建议使用默认安装路径），单击“**下一个**”按钮，弹出如图6所示的“**选择程序文件**”夹对话框，可以接受默认文件夹，也可以根据需要新

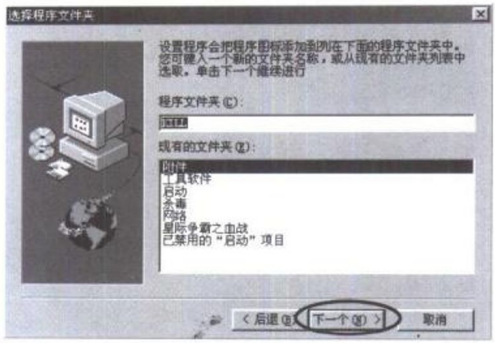


图 6　选择程序文件夹

建一个文件夹。

（6）单击“**下一个**”按钮，弹出如图7所示的“**开始复制文件**”对话框，在对话框中单击“**下一个**”，系统即开始安装软件。

（7）文件复制结束后，将弹出如图 8 所示的“**重新启动 Windows**”对话框，选择“**是**”或“**否**”以后单击“**结束**”按钮，完成安装。

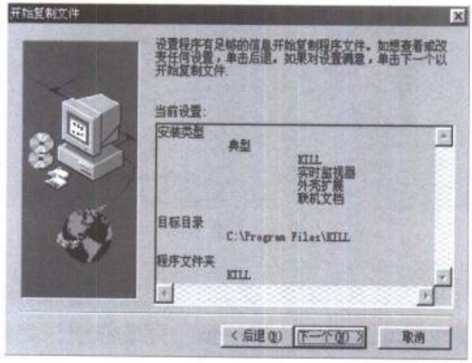


图 7　复制文件对话框

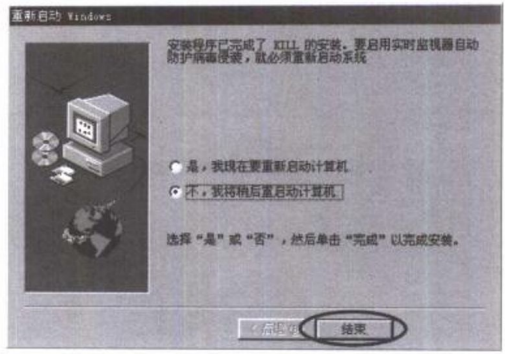


图 8　重新启动 Windows 对话框

（8）重新启动机器后KILL将自动启动，弹出如图9所示的对话框，提示安装成功，可进行其他的工作。

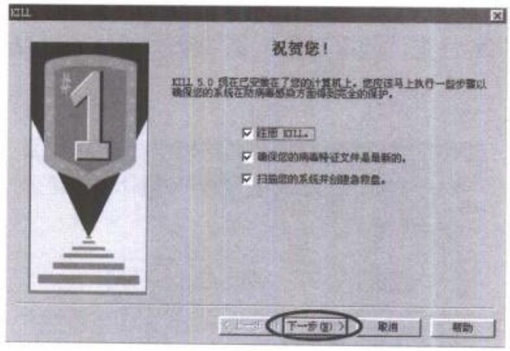


图 9　安装成功

（9）为了以后处理问题的安全可靠，我们建议用户应将选择项列表中的三项都打勾，单击“**下一步**”完成注册、更新病毒库和创建急救盘的工作。

4.启动KILL和创建急救盘

KILL2000在我们的电脑上安装完成后，我们要介绍一下怎样启动KILL，为我们的电脑提供安全保障。

其方法是：

将KILL for Windows 95/98光盘插入光盘驱动器中，如图10所示，单击“**开始>程序>KILL>KILL**”，应用程序将自动启动并打开扫描程序主窗口，如图11所示。

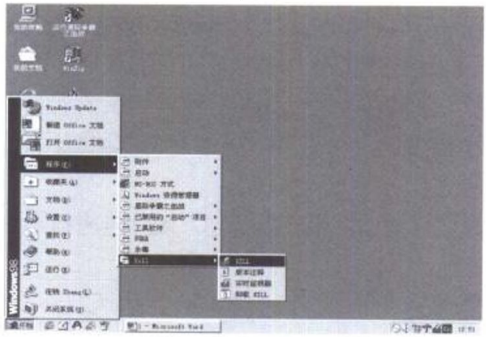


图10 启动KILL 2000

注 意

每次启动程序时，都需要将KILL for Windows 95/98光盘插入光盘驱动器中，以便KILL程序搜索到必要的信息。